THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:	
A BLACK APPLE IPHONE CURRENTLY IN THE CUSTODY OF THE FBI AT EVIDENCE NUMBER 1B8	Magistrate No. 25-1020
A WHITE APPLE IPAD CURRENTLY IN THE CUSTODY OF THE FBI AT EVIDENCE NUMBER 1B9	Magistrate No. 25-1021

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Abigail Patcher, being duly sworn, hereby depose and state the following:

I. INTRODUCTION

1. This affidavit is made in support of search warrants for an Apple iPhone and iPad, currently in the custody of the FBI as described in Attachments A-1 and A-2. As detailed herein, there is probable cause to believe that these devices contain records, instrumentalities, contraband, fruits, and/or evidence that EDWARD ARTHUR OWENS, JR. violated Title 18, United States Code, Sections 875(c) (prohibiting transmitting in interstate or foreign commerce any communication containing a threat to injure the person of another), as well as 1001 (prohibiting making any materially false, fictitious, or fraudulent statement or representation), as described in Attachment B.

2. I have served as a Federal Bureau of Investigation Special Agent since July of 2011. As a Special Agent with the FBI, I am an "investigative or law enforcement officer" of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18.

3. I am currently assigned to the Public Corruption and Civil Rights squad in the FBI Pittsburgh Division. In this capacity, I am charged with investigating possible violations of federal criminal law. By virtue of my FBI employment, I perform and have performed a variety of investigative tasks, including functioning as a case agent on both Public Corruption and Civil Rights investigations. I have received training and have gained experience in the conduct of federal criminal investigations, the execution of federal search and seizure and arrest warrants, and the identification, collection, and review of voluminous computer-related evidence.

4. The facts set forth in this affidavit are based on my personal knowledge, the knowledge obtained during my participation in this investigation, the knowledge obtained from other individuals, including other law enforcement personnel, review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the requested search warrants, this affidavit does not set forth each and every fact that I have learned during the course of this investigation.

5. For the reasons set forth herein, there is probable cause to believe that, on or about May 20, 2025, in the Western District of Pennsylvania, the defendant, OWENS, knowingly and willfully transmitted in interstate commerce a communication containing a threat to injure the person of a local public official (Victim 1). As provided below, OWENS communicated to Victim 1 via Facebook Messenger to Victim 1's personal Facebook account the following statement: "We're coming for you [emoji of person raising right hand] [German flag emoji] be afraid. Go

back to Israel or better yet, exterminate yourself and save us the trouble. 109 countries for a reason. We will not stop until your kind is nonexistent."[1]

II. STATUTORY PROVISIONS

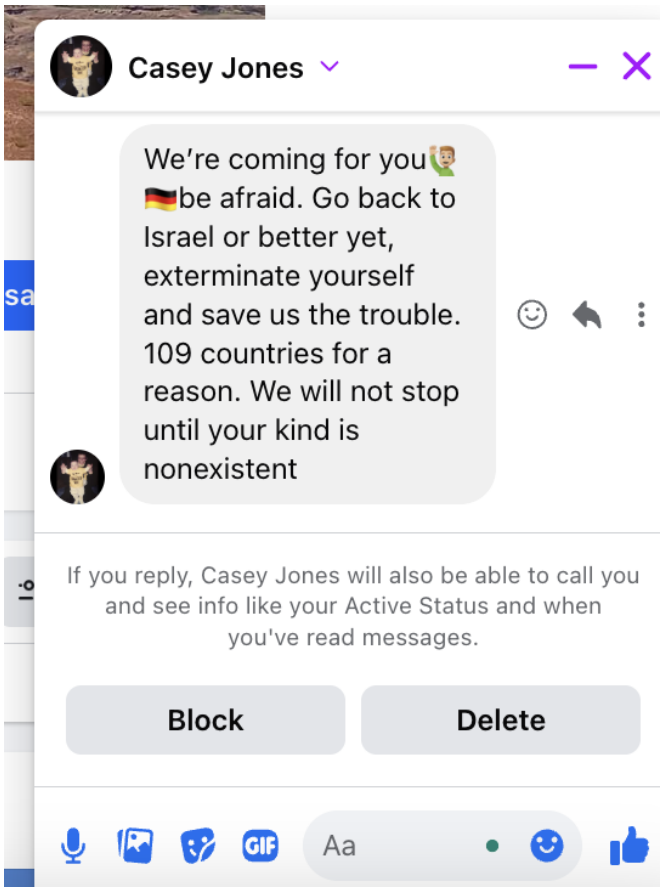
6. Title 18, United States Code, Section 875(c), makes it a federal felony offense to "transmit in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another . . . ."

III. PROBABLE CAUSE

7. The allegations in this affidavit pertain to a recent threat using electronic communication services by OWENS, who resides in the Western District of Pennsylvania.

8. On May 23, 2025, I received a true threat complaint from the Duty Agent. According to the complainant (Victim 1), the threat was directed to Victim 1's personal Facebook Messenger account. Victim 1 provided the below picture of the Facebook Messenger message Victim 1 received:

[1] According to the Anti-Defamation League, the reference to "109 countries" is an antisemitic claim that Jews have been expelled from 109 different countries, which antisemites use to support a call to expel Jews from other countries and otherwise to promote hatred.



9. While the public display name associated with this account was "Casey Jones," this message was sent by Facebook account identifier "teddy.owens.129".

10. On May 23, 2025, I interviewed Victim 1, whose identity is known to law enforcement. According to Victim 1, Victim 1 does not know the user of this account. Victim 1 advised that the message was delivered to Victim 1's Messenger account on May 20, 2025, at approximately 7:23 p.m., but Victim 1 did not see the message until May 22, 2025. Victim 1 is a local public official, who engages regularly with the public to include attending events such as parades and other large gatherings. Victim 1 communicated to law enforcement that Victim 1 felt threatened by the message and expressed concern for Victim 1's safety as well as for the safety of those in Victim 1's office and Victim 1's home.

11. On May 23, 2025, I issued an emergency request to Meta for subscriber information associated with the Facebook screen name "Casey Jones" and username "teddy.owens.129". On May 24, 2025, I received information from Meta which provided the following Facebook account information associated with the screen name "Casey Jones" and account identifier "teddy.owens.129":

Email Address:	Jmoney5921@gmail.com (verified) Teddy.owens.1297@facebook.com (verified)
Date of Birth:	MM/DD/1995[2]

12. Additionally, Meta provided the IP address information for identifier "teddy.owens.129" from May 18, 2025, through May 23, 2025, which was provided in Coordinated Universal Time (UTC).[3] Meta provided multiple IP addresses, however the following IP addresses are specific to May 20, 2025, the date the threat was sent to Victim 1:

IP Address	**Date**	**Time**
2601:0547:c983:0f20:2ddb:c9d4:4a08:c4b8	2025-05-20	23:26:33 UTC (7:26:33 PM EDT)
2601:0547:c983:0f20:f158:9576:fe20:b49b	2025-05-20	18:09:59 UTC (2:09:59 PM EDT)

13. Based upon my training and experience, I know that Meta's Facebook social media platform utilizes data centers to process Internet activity, including Facebook Messenger activity, occurring on its platform. On May 28, 2025, I communicated with Meta's Director of Law Enforcement Outreach regarding whether Meta utilizes data centers in the Commonwealth of Pennsylvania. This individual explained that Meta maintains a listing of all its data centers in the

[2] Please note that the Meta account information provided the complete date of birth associated with this account, which has been excluded from this affidavit but is known to me. As discussed herein, the date of birth contained in the account information is the same as OWENS' date of birth from other sources, including his Pennsylvania Department of Transportation records.

[3] Eastern Daylight Time (EDT) is currently UTC minus 4.

United States on the following publicly available website: <https://datacenters.atmeta.com/us-locations/>. I accessed and reviewed this website on May 28, 2025. According to Meta, Meta does not have a data center in the Commonwealth of Pennsylvania. Accordingly, based upon my training and experience, OWENS' message to Victim 1 would have traveled in interstate commerce from Elizabeth, Pennsylvania, to a Meta data center located outside of Pennsylvania, and then from that data center to Victim 1's device containing Victim 1's Facebook Messenger application.

14. Upon receiving the subscriber information from Meta, I determined the listed IP address resolved to Comcast. I then issued two emergency disclosure requests (EDR), one to Google Inc., for subscriber information associated with email address "jmoney5921@gmail.com" and the other to Comcast for the IP address associated with Meta.

15. On May 24, 2025, I received subscriber information from Comcast for these IP addresses, which provided the name, address, and telephone number associated with these IP addresses. These Comcast records disclosed the specific name and address of the Comcast subscriber, which are known to me but excluded from this affidavit for privacy reasons. The subscriber address is a residential address in Elizabeth, Pennsylvania. The subscriber's name will be referred to herein as Witness 1. FBI agents interviewed Witness 1 on May 25, 2025. As discussed below, Witness 1 informed investigators that OWENS resides with Witness 1 at Witness 1's residence in Elizabeth, PA. A review of Witness 1's Facebook profile shows Witness 1 pictured with OWENS.

16. Additionally, Google responded with subscriber information associated with Jmoney5921@gmail.com

Name:	TED OWENS
Phone Number:	###-###-1312[4]

17. In addition to the above listed IP address from the threatening communication, Meta also provided additional IP information for Facebook account teddy.owens.129. This IP information shows that Facebook account teddy.owens.129 used Witness 1's Comcast IP address as recently as May 23, 2025, the date of the request to Meta.

18. Accordingly, I believe that OWENS is the Facebook account holder who sent this threatening communication via interstate commerce to Victim 1.

19. Additionally, on May 25, 2025, I along with other law enforcement officers seized OWENS' cell phone from his person pursuant to a federal search warrant. Magistrate Judge Kezia O. L. Taylor authorized this search warrant at Magistrate No. 25-953. At the time, OWENS was with Witness 1. Investigators then conducted separate voluntary interviews with Witness 1 and OWENS.

20. During OWENS' voluntary interview, he accessed his Facebook Messenger application on his phone in my presence and showed me that he knowingly utilized the Messenger application at approximately 10:13 p.m. on May 20, 2025, in connection with a Facebook Marketplace exchange. In so doing, he also located the threatening communication in his Facebook Messenger application also from May 20, 2025. He initially denied sending the threatening communication. OWENS initially claimed his Facebook account must have been hacked, but later clarified that was not the case.

21. After confronting OWENS with information regarding IP addresses associated with his Facebook account, OWENS stated that he must have been "black-out drunk" and

[4] Google provided the full phone number associated with this account.

acknowledged the message was sent from his account and said he should take responsibility for the message, even though he did not recall sending it. After the interview ended, OWENS voluntarily reapproached the agents and reiterated he wanted to take responsibility for the message because he was a drunk. He denied knowing who Victim 1 was and further denied harboring any biases or ill will towards any groups of people. He acknowledged living with Witness 1 since 2024 and indicated they are the only two people residing at the residence.

22. OWENS told investigators that he possessed a Pennsylvania concealed carry weapons permit. However, he claimed that he did not have any weapons where he was living in Elizabeth, PA. He acknowledged that his family has firearms, so he has fired firearms with his family.

23. Witness 1 was also interviewed. Witness 1 acknowledged being in a relationship with OWENS since late spring of 2023 and living with OWENS at Witness 1's residence in Elizabeth, PA, for more than a year. Witness 1 indicated Witness 1 spent the evening of May 20, 2025, at Witness 1's residence with OWENS and did not observe him to be intoxicated.

24. Witness 1 confirmed OWENS has antisemitic views and has previously said "upsetting things" concerning Jewish people. Witness 1 stated that OWENS' antisemitic comments were not frequent at first; however, his comments were becoming more frequent. For example, OWENS made statements to Witness 1 such as "Jews control everything" and "Jews control the news." At one point, while watching a video of Adolf Hitler, OWENS turned to Witness 1 and said, "He [Hitler] did not do anything wrong." OWENS follows local politics. Witness 1 also asserted that OWENS sent Witness 1 antisemitic content on social media.

25. On May 26, 2025, I received a voicemail from OWENS using the number ending in 1312 (the same number associated with his Google account). I listened to the voicemail and understood the recording to state the following:

> Hi Abigail, this is Edward Owens calling I uh just wanted to touch base with you follow up a day later here and uh, and you know I just wanted to reiterate that you know I have, I have to take responsibility for what was said on my accounts. You know I uh I have my issues and what not, and that's no excuse and uh, that you know I need to own up for what I did regardless of whether or not uh you know the state of mind I was in. I um, I need to take responsibility and um I just wanted to make sure that I reiterated that, and uh you know I do apologize I'm, I'm not an extremist of any kind. I'm not part of any groups, I'm sure you'll see that once you go through my phone. I'm just a keyboard warrior as you put it, I uh you know when you, you get in those ways of getting rage baited on line and you know you just, you lash sometimes and you say thing you don't mean, and I, I really, really messed this one up. So yea, I just, yea I wanted to reiterate again that I you know I take responsibility for what was said on my account and uh yea, I apologize. So I uh I got a got a new phone here, that's why I am able to call you off my number. So if you get this and want to talk about anything, feel free to give me a call. I'll uh I know this is your number now, so I'll, I'll be sure to answer if I see your number pop up. So again, I just uh, I wanted to, I wanted to reiterate that uh that point that uh no excuse for what I said regardless of my state of mind. It uh not something that should ever be said, and it's not something that I truly believe. So again I apologize. Um enjoy your Memorial Day, and uh talk to you soon. Bye.

26. A preliminary review of OWENS' cell phone seized on May 25, 2025 revealed the following:

a. A text message, dated May 20, 2025 (the same day he communicated the true threat) to an individual whom, based upon other communications appears to be OWENS' friend, stating:

b. Photographs of two pistols, as pictured below:

c. Search history revealing the following inquires:

C. "nyc synagogue," from May 21, 2025;

D. "dancing israelis," from May 25, 2025;

E. "lowes shooting may 29th 2021," from May 11, 2025; and

F. "adolf hitler," date unknown.

27. On May 30, 2025, Magistrate Judge Patricia L. Dodge authorized a criminal complaint for OWENS for violating Title 18, United States Code, Section 875(c), based upon the affidavit and application filed at Magistrate No. 25-991. That morning FBI agents arrested OWENS at the FBI field office in Pittsburgh, PA.

28. OWENS was read and voluntarily waived his *Miranda* rights. During the resulting interview, he stated the following:

a. He possessed an assault rifle, pistol, and .22 caliber rifle, which he claimed were all locked at his mother's residence.

b. He was not sure if he deleted any messages or comments from Facebook or other social media websites after law enforcement seized OWENS' cell phone on May 25, 2025. When specifically asked if he accessed his Facebook account after agents spoke with him on May 25, 2025, OWENS stated he had accessed it. Agents again asked if he deleted anything from his accounts on his new phone and OWENS again advised that he could not remember and was not sure.

c. OWENS advised he does not interact with anyone who has extremist views.

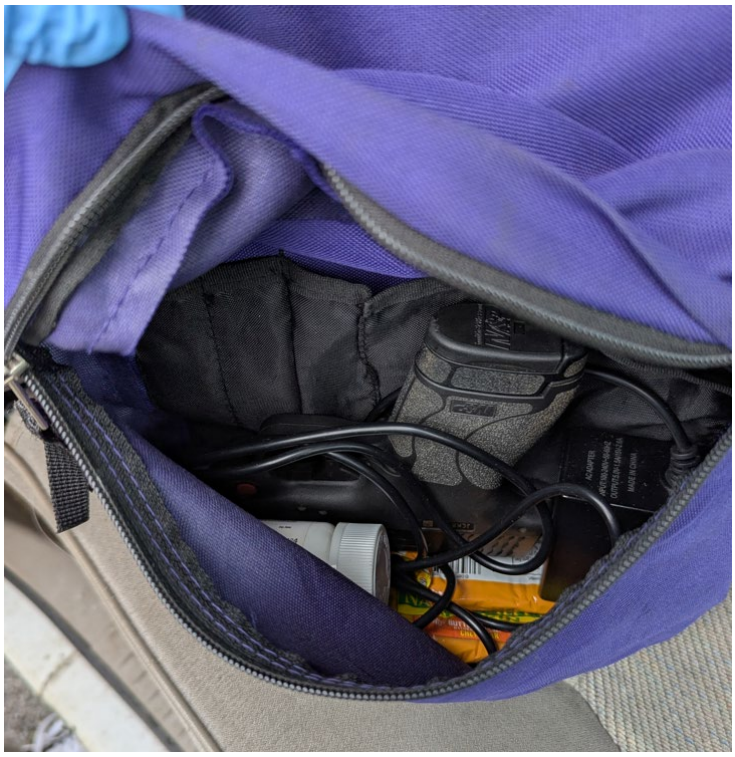
29. Following his arrest, OWENS' mother provided the United States consent to search the vehicle that OWENS drove to the FBI's Pittsburgh office on May 30, 2025. OWENS was the sole occupant of the vehicle. OWENS' mother is the registered owner of this vehicle pursuant to Pennsylvania Department of Transportation records. Of note, the vehicle OWENS was driving remained parked at the FBI field office in Pittsburgh, PA, in view of the guard building, which was manned while the vehicle remained so parked. No third-party was observed entering or interacting with the vehicle. Below is a picture of the vehicle parked in the FBI parking lot.

30. Following OWENS' mother's consent, the FBI searched the vehicle and located the following notable evidence:

a. A Butler-county issued Pennsylvania concealed carry weapons permit issued to OWENS, which was located in the vehicle's driver-side front door.


SP 4-129(1-2010)
PENNSYLVANIA LICENSE TO CARRY FIREARMS
☒ NEW ☐ RENEW
☐ DUPL / CORRECTION
NO. 10-00040005
1. NAME(LAST) (FIRST) (MIDDLE) (JR.,ETC.)
OWENS, EDWARD ARTHUR JR
2. ADDRESS
[redacted]
3. Point Of Contact Phone Number
[redacted]3802
(FOR LAW ENFORCEMENT USE ONLY)
4. DATE ISSUED
7/16/2019
5. DATE EXPIRES
7/16/2024
6. REASON TO CARRY
Self Defense
7. DOB
[redacted]1995
8. HGT
603
9. WGT
170
10. EYES
BLU
11. HAIR
BRO
12. SEX
M
13. RACE
W
14. U.S. CITIZEN
Y
15. COUNTRY OF CITIZENSHIP
US
16. IMMIGRATION ID NO. (IF APP)
17. SIGNATURE OF LICENSEE
18. SIG OF ISSUING AUTHORITY
19. SHERIFF OR CHIEF OF POLICE OF
Butler

b. A loaded Smith & Wesson M&P 9 Shield 9mm caliber semi-automatic pistol including one in the chamber, which was in the front pocket of a backpack on the front-passenger seat. Commonwealth of Pennsylvania records indicated that this firearm is registered to Edward Arthur Owens, Jr., with the same date of birth as OWENS.



c. Approximately 265 rounds of 9mm caliber ammunition were recovered from a Trader Joe's bag, which was located behind the front driver's seat, in addition to those rounds loaded in the above-pictured pistol.

a. Approximately 400 rounds of .22 Long Rifle caliber ammunition were also recovered from the Trader Joe's bag found behind the front drivers seat.

b. Empty AR-15-style magazines for 5.56 caliber ammunition, including such a magazine capable of accepting 60 rounds of 5.56 caliber ammunition, which were located in the Trader Joe's bag behind the front seats.

SEARCH AND SEIZURE OF CERTAIN DIGITAL DEVICES

31. This affidavit is in support of an application for search warrants seeking authorization to search the contents of certain digital devices described in Attachments A-1 and A-2, which are capable of connecting to Facebook. Based upon my training and experience, I know

that individuals who engage in criminal activity, including communicating online threats, often use such digital devices to facilitate their actions. Additionally, my initial review of OWENS' phone seized on May 25, 2025, revealed online activity evidencing OWENS' bias against Jews, which gives important context to his threat.

32. Based on my training and experience, I am aware that Facebook is a social media site, and that posting and sending messages and friend requests requires the use of a digital device such as a tablet or cellular phone that is connected to the Internet. Based upon my training and experience, I know that Facebook can syncronize messages and other communucations across a user's devices that are logged into the user's Facebook account, such as the devices identified in Attachments A-1 and A-2.

33. Finally, OWENS possessed two pictures of firearms on the cell phone seized on May 25, 2025. This is in the context of one of the pictured pistols being located in the vehicle he was driving, despite telling investigators that his firearms were secured at his mother's residence. Given these facts, digital evidence of firearms possession is likely to be found on the devices subject to this application, which provides critical context to his threat and related actions, as well as his false statement to law enforcement regarding the location of his weapons.

34. Accordingly, evidence of the alleged offenses is likely to be found on the digitial devices described in Attachments A-1 and A-2.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

35. Based on my knowledge, training, and experience, I know that certain portable digital devices capable of connecting to Facebook (i.e., a cell phone and tablet) can store information for long periods of time. Similarly, things that have been viewed via the Internet are

typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

36. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of such devices consistent with the applied-for warrants. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrants.

37. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

38. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled

environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

39. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment and can require substantial time.

40. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non- text format. Documents printed by

a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

41. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio

application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

42. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, I request permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

43. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises.

44. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

a. Law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B, which are currently in FBI custody. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

b. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

c. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

IV. CONCLUSION

45. For all of the foregoing reasons, I respectfully submit that there is probable cause to believe that EDWARD ARTHUR OWENS, JR. violated Title 18, United States Code, Sections 875(c) and 1001 and that records, instrumentalities, contraband, fruits, and/or evidence of such violations will be found on the devices described in Attachments A-1 and A-2.

The above information is true and correct to the best of my knowledge, information and belief.

/s/Abigail Patcher
Special Agent
Federal Bureau of Investigation

The Affiant attested to this Affidavit
by telephone pursuant to FRCP 4.1(b)(2)(A)
this 3rd day of June, 2025.

_____
HONORABLE MAUREEN P. KELLY
United States Magistrate Judge

ATTACHMENT A -1

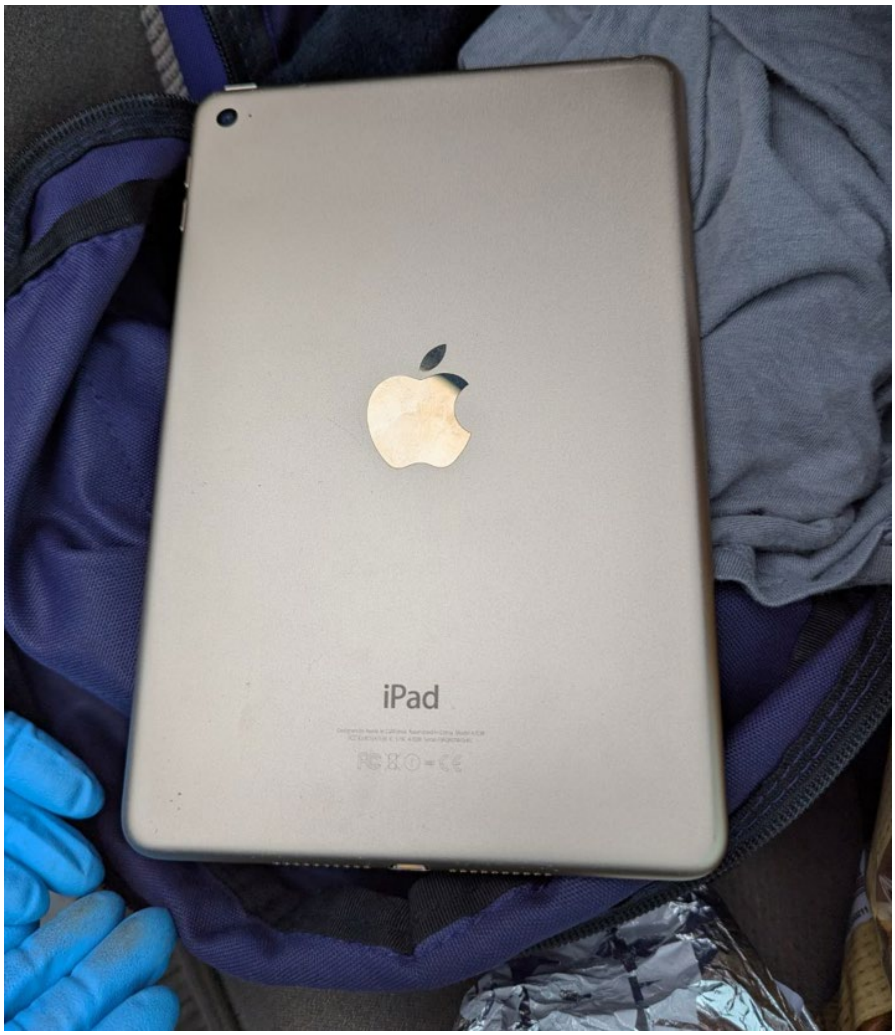
Property to be Searched

The property to be searched is a black Apple iPhone seized on May 30, 2025, and currently in the custody of the FBI at 3311 East Carson Street, Pittsburgh, PA 15203 under evidence number 1B8.

ATTACHMENT A-2

Property to be Searched

The property to be searched is a white Apple iPad seized on May 30, 2025, and currently in the custody of the FBI at 3311 East Carson Street, Pittsburgh, PA 15203 under evidence number 1B9.



ATTACHMENT B

Information to be Seized

1. All information that constitutes records, instrumentalities, contraband, fruits, and/or evidence related to violations of 18 U.S.C. §§ 875(c) (transmitting a threat to injure another in interstate commerce) and 1001 (making a materially false statement or representation) by EDWARD ARTHUR OWENS, JR., including:

a. Communications representing threats to any individual utilizing interstate commerce;

b. All records and information involving firearms, firearm parts, ammunition, or body armor;

c. Records and information indicative of hostility towards Victim 1 or Jewish persons;

d. Records and information relating to membership in antisemitic groups or organizations;

e. Records and information relevant to the state of mind of OWENS with respect to the crime under investigation;

f. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

g. Evidence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

h. Evidence of the lack of such malicious software;

i. Evidence indicating how and when the device was accessed or used to determine the chronological context of access, use, and events relating to crime under investigation and to the user;

j. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

k. Evidence of the times the device was used;

l. Records and information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. Contextual records and information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage or filetype. This warrant authorizes a review of electronically stored information, communications, other records, and information disclosed pursuant to this warrant in order to locate evidence described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.